THE UNITED NATIONS AND THE REGULATION OF CYBER-SECURITY

CHRISTIAN HENDERSON*

in
N. Tsagourias and R. Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015)

1. Introduction

The importance of cyberspace in today's interconnected and highly complex world cannot be overstated. It has become central for the smooth running of the world economy, the carrying out of daily business transactions, political communications, as well as for social networking. The late 1990s saw an exponential growth in the use of the Internet with over 2.5 billion users across the world today.[1]

While in general the development of cyberspace has undoubtedly proved to be in an immensely positive development, its rise has also been accompanied by a more sinister side, in that the development of information and communication technologies (ICTs) has given rise to various risks to individuals, societies and states more broadly. Although 'governments have attempted to address these issues by creating national-level mechanisms, the very transnational nature of cyberspace has forced the international community to debate and form norms or rules that should promote good behavior in cyberspace.'[2] Activity in this respect has been occurring in various institutional and regional forums for some time. For example, the OSCE's Budapest Convention on Cybercrime entered into force in 2004 and is seen as a positive precedent in the regulation of this element of cyber-security.[3]

Activity within the UN to address cyber-security issues begun when the Russian Federation introduced a draft resolution into the UN General Assembly (UNGA) in 1998 on '[d]evelopments in the field of information and telecommunications in the context of international security'.[4] Subsequent initial activity within the UN proved somewhat 'dull without much movement … towards dealing with issues in cyberspace'.[5] Yet, 'mounting reports of disruptions and the increasing potential of cyber attacks disturbing the peace in the real world led countries to examine these

* The author wishes to thank April Longstaffe for her research assistance in preparing this chapter.
[1] World Internet Usage and Population Statistics, Internet World Stats, 30 June 2012, available at http://www.internetworldstats.com/stats.htm.
[2] R. Prakesh and D.M. Baruah, 'The UN and Cyberspace Governance', *ORF Issue Brief*, February 2014, at 1, available at http://orfonline.org/cms/export/orfonline/modules/issuebrief/attachments/issuebrief68_1394871027354.pdf.
[3] Council of Europe, Convention on Cybercrime, 23 November 2001, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG.
[4] UNGA A/RES/53/70, 4 December 1998.
[5] Prakesh and Baruah, supra n.2, at 1.

challenges more seriously within the UN.'[6] Indeed, the Distributed Denial of Service Attacks (DDoS) on Estonia (2007) and Georgia (2008), the Stuxnet worm attack upon Iran (2010) and the Edward Snowden revelations (2013) regarding the use of ICTs by states to spy upon one another brought to light in dramatic fashion the realities of cyberspace being used in unscrupulous ways and raised the profile of cyber-security on the UN's agenda. In light of these events, it is fair to say that '[t]he issue of cyber security is quickly making its way up the agenda of global public policy issues demanding attention.'[7]

While one might, nonetheless, take the view that '[t]here has been only limited U.N. action on the issue of cyber-security',[8] this is arguably down to the fact that there have been fundamental differences on fundamental issues between Eastern and Western states. The main sticking points appear to be whether there should be a free flow of information or whether there should be governmental restrictions upon it; whether the focus should be on economic espionage and criminal activity or upon the use of cyberspace to carry out attacks; and whether existing international law applies to cyber-security issues or whether new rules and norms need to be developed, perhaps in the form of a new treaty. In this respect, the UN 'has been working for over a decade to eliminate these differences and create a mechanism to ensure the security and stability of cyberspace.'[9] As this chapter will attempt to highlight, the UN, through its work on both issues of cyber warfare and cyber crime,[10] is now moving with some momentum.

The UN's activities in this area are highly fragmented with a very complex system of bodies dealing with it and with expertise scattered throughout the system meaning that a full analysis is beyond the limited scope of this chapter. The purpose of this chapter is thus twofold. Its primary aim is to provide an overview of UN activities and initiatives concerning the regulation of cyberspace and cyber-security. The chapter also attempts to discern whether any regulatory norms have emerged in this field of activity. While it will touch upon issues such as the use of force in cyberspace and cybercrime, these have been dealt with in-depth in other chapters of this Handbook.[11]

2. The United Nations General Assembly

While the UNGA may in several respects be considered as the second organ of the UN in regards to the maintenance of international peace and security, and can only make recommendations as opposed to legally oblige states to take a particular course of action,[12] it has nonetheless been central in the process of norm development in the

[6] Ibid., at 1-2.
[7] P. Meyer, 'Cyber Security Takes the Floor at the UN', *opencanada.org*, 12 November 2013, available at http://opencanada.org/features/the-think-tank/comments/cyber-security-takes-the-floor-at-the-un/.
[8] O.A. Hathaway *et al*, 'The law of cyber-attack' (2012) 100 *California Law Review* 817, at 865.
[9] Prakesh and Baruah, supra n.2, at 1.
[10] While there is an obvious overlap between the two, cyber-warfare is mainly concerned with how '[information] technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States' (see A/RES/53/70) while cyber-crime, on the other hand, is concerned in general with 'the criminal misuse of information technologies' (See A/RES/55/63).
[11] See Chapters ????.
[12] Arts 10-17, UN Charter (1945).

context of cyber-security. The main discursive work of the UNGA occurs in its various committees, of which there are six.[13] Three out of the UNGA's six committees have met to discuss the issue of cyber-security and negotiate draft resolutions in relation to it, which were then submitted to the plenary for adoption at the UNGA's annual session each year.

2.1. The First Committee

The First Committee of the UNGA – the Disarmament and International Security Committee – is concerned with disarmament and related international security questions and was the first committee to engage with issues of cyber security. Indeed, the issue of information security has been on the agenda of the UN since 1998 when the Russian Federation introduced its draft resolution in the First Committee on '[d]evelopments in the field of information and telecommunications in the context of international security', which was subsequently adopted without a vote.[14] This resolution built upon previous work on the '[r]ole of science and technology in the context of security, disarmament and other related fields'[15] and has been subsequently introduced every year since. Its key elements are that it:

- mentions the dual use of developments in the area and the military potential of ICTs for the first time;[16]
- expresses concern about the use of such technology 'inconsistent with the objectives of maintaining international stability and security';[17]
- noted the need for broad international cooperation;[18]
- called upon Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security;[19]
- mentions the need to prevent cyber-crime and cyber-terrorism;[20] and
- invitesd Member States to inform the UN Secretary-General of their views regarding 'definitions and the development of 'international principles'.[21]

In introducing this resolution, Sergey Ivanov, Minister of Defense of the Russian Federation from 2001 to 2007, stated that 'Russia want[ed] to develop international

[13] The six main committees of the UNGA are: First Committee (Disarmament and International Security Committee), Second Committee (Economic and Financial Committee), Third Committee (Social, Humanitarian and Cultural Committee), Fourth Committee (Special Political and Decolonization Committee), Fifth Committee (Administrative and Budgetary Committee), and Sixth Committee (Legal Committee).
[14] UNGA A/RES/53/70, 4 December 1998.
[15] UNGA A/53/576, 18 November 1998.
[16] UNGA A/RES/53/70, supra n.14, preamble.
[17] Ibid.
[18] Ibid.
[19] Ibid., para.1.
[20] Ibid., preamble.
[21] Ibid., at para. 2.

law regimes for preventing the use of information technologies for purposes incompatible with missions of ensuring international stability and security'. [22] However, the US has always taken, and as noted below continues to take, the position that '[t]he same laws that apply to the use of kinetic weapons should apply to state behaviour in cyberspace' while trying to increase cooperation among law enforcement agencies.[23] In this respect, the original push by Russia for what was perceived as an international treaty was met with suspicion by the US and EU states in the belief that a treaty could be used to limit the freedom of information under the guise of increasing information and telecommunications security.[24]

Yet, while the idea of an international treaty to regulate cyberspace was divisive, this did not impact upon general support for the resolution itself. Indeed, in 2005, an important change took place in the First Committee in that the draft resolution that had been introduced into the UNGA annually by Russia was adopted but went to a recorded vote.[25] The US was the only state to vote against the resolution.[26] Arguably as a result of US opposition the draft resolution introduced in 2006 was no longer sponsored by Russia alone, but also co-sponsored by China, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Myanmar, Tajikistan, and Uzbekistan.[27] Additional states joined as co-sponsors in subsequent years.[28]

However, after President Obama had succeeded President Bush as President of the United States in 2009 the US adopted a 'reset' policy not only with regards to Russia but also with the UN itself.[29] The US subsequently initially agreed to discuss cyber-warfare and cyber-security with representatives of the First Committee.[30] In January 2010, President Obama then presented a position paper with the objective of bringing the two parties together[31] and, later that year, the US went on to reverse its long-time policy position towards the annually introduced resolution and for the first time became a co-sponsor of the draft resolution.[32] Yet, this did not mean that the US had fully aligned itself with the position of the Russian Federation. On the contrary, there were two key changes to the 2010 draft from the original draft of the resolution:

- omission of the reference to, and attempts to come up with, definitions that were perceived as a first-step towards a cyber arms control treaty; and

[22] C.A. Ford, 'The Trouble with Cyber Arms Control', (2010) *The New Atlantis: A Journal of Technology & Society* 52, at 65.
[23] Ibid., at 67.
[24] China was initially relatively quiet on this issue but subsequently appeared to align itself with the position of Russia.
[25] See UNGA A/60/452.
[26] Ibid.
[27] See UNGA A/C.1/61/L.35.
[28] UNGA A/61/389.
[29] T. Maurer, 'Cyber Norm Emergence at the United Nations: An Analysis of the Activities of the UN Regarding Cyber-Security', Belfer Center for Science and International Affairs (Discussion Paper #2011-11), September 2011, at 23, available at http://belfercenter.hks.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.
[30] Ibid.
[31] Ibid.
[32] Ibid., at 24.

- substitution of the reference to 'international principles' with references to what was perceived as more benign language in the form of 'international concepts' and 'possible measures'.

While the resolution, albeit with certain amendments,[33] continues to be introduced in the UNGA each year, the main work of the First Committee and the focus of its resolutions has centered on the work of several Groups of Governmental Experts (GGEs), which will be addressed below. Before doing so, it should not be forgotten that work on the issue of cyber-security has also been undertaken in the Second and Third Committees of the UNGA.

2.2. The Second Committee

The Second Committee – the Economic and Financial Committee – is concerned with economic questions, so might not immediately be seen to be relevant in discussions regarding cybersecurity. However, while it is fair to say that the First Committee has tended to focus upon issues of cyber warfare and the Third Committee upon issues of cyber crime,[34] the Second Committee has addressed both through its 'Global Culture of Cyber-security' initiative. The three resolutions of the UNGA's Second Committee on this initiative are concerned with both cyber warfare and cyber crime and all reference the resolutions of both the First and Third Committees.[35]

In light of the decision of the Third Committee to no longer focus on cyber-crime, the US introduced a new draft resolution in the Second Committee in 2002 entitled '[c]reation of a global culture of cyber-security'. While initially co-sponsored by Japan, Australia and Norway, after a number of revisions to the original draft 36 other Member States joined as co-sponsors, including the Russian Federation.[36] Indeed, one of the revisions was to introduce references to resolutions adopted within the UNGA's First Committee, which had, as noted above, been mainly drafted by Russia. It was subsequently adopted without a vote.[37]

There were several significant elements to this original resolution. First, in order to attract the support of many developing countries the resolution had a focus on capacity-building, which was something that the GGEs subsequently put much store by.[38] The preamble noted, for example, that 'gaps in access to and the use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal use of information technology' while the final operative paragraph '[s]*tresse*[d] the necessity to facilitate the transfer of information technology and capacity-building to developing countries, in order to help them to take measures in cybersecurity.'[39] Secondly, the resolution had annexed to it a series

[33] For example, the inclusion of references to the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies, the need to address threats consistent with the free flow of information, and references to the various initiatives of the UN Secretary-General and the responses of Member States.
[34] See sections 2.1 and 2.3 of this chapter respectively.
[35] UNGA A/RES/57/239; UNGA A/RES/58/199; UNGA A/RES/64/211.
[36] UNGA A/57/529/Add.3. China did not co-sponsor the resolution.
[37] UNGA A/RES57/239.
[38] See section 2.4 of this chapter.
[39] UNGA A/RES/57/239, para.5

of '[e]lements for creating a global culture of cybersecurity', which Member States were invited to take into account.[40] These elements covered nine areas: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment.[41] While these were titled 'principles', as opposed to 'elements', in the original draft, along with the fact that they were originally due to be 'adopted' but which was later changed so that Member States were to simply take them 'into account', they nonetheless arguably represented a certain consensus regarding regulatory norms in the context of cyber security.[42]

These 'elements' were expanded upon in the second resolution of the Second Committee on the creation of a global culture of cybersecurity, that was adopted by the UNGA in January 2005, with the addition of the 'protection of critical information infrastructures'. [43] These elements included actions such as having emergency networks regarding cyber-vulnerabilities, threats and incidents, [44] examining information infrastructures and the interdependencies between them,[45] promoting partnerships, including the sharing of information, between public and private stakeholders,[46] having adequate substantive and procedural laws and trained personnel to enable effective investigations and prosecutions in response to attacks,[47] and engaging in international cooperation to secure critical information infrastructures.[48] The resolution, and the included elements, was co-sponsored by 69 countries, this time including China but not Russia.[49] Nonetheless, the broadening of the elements could be perceived as a progressive step towards the formation of a regulatory cyber-security regime.[50]

The final resolution was adopted in 2010 after the US policy shift.[51] It was sponsored by the US on behalf of 39 states, although not Russia or China. This resolution was titled the '[c]reation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures' and included an annex outlining a '[v]oluntary self-assessment tool for national efforts to protect critical information infrastructures'. This is explained as 'a voluntary tool that may be used by Member States, in part or in its entirety, if and when they deem appropriate, in order to assist in their efforts to protect their critical information infrastructures and strengthen their cybersecurity.'[52] These include '[t]aking stock of cybersecurity needs and strategies', '[s]takeholder roles and responsibilites', '[p]olicy processes and participation', '[p]ublic-private cooperation', '[i]ncident management and recovery', '[l]egal frameworks', and '[d]eveloping a global culture of cybersecurity'.[53] Notably, these

[40] Ibid., para.3.
[41] Ibid., appendix.
[42] Maurer, supra n.29, at 44.
[43] UNGA A/RES/58/199. See appendix for the expanded elements.
[44] Ibid., annex, element 1.
[45] Ibid., annex, element 3.
[46] Ibid., annex, element 4.
[47] Ibid., annex, element 9.
[48] Ibid., annex, element 10.
[49] UNGA A/58/481/Add.2.
[50] Maurer, supra n.29, at 44.
[51] UNGA A/RES/64/211.
[52] Ibid., n.2.
[53] Ibid., annex.

highlight the importance of cooperation among states, including through 'international information-sharing and collaboration'.[54]

2.3. The Third Committee

The Third Committee – the Social, Humanitarian and Cultural Committee – is, as its title suggests, concerned mainly with social and humanitarian issues, but in the context of cyber-security with cyber crime. Two years after the Russian Federation introduced its resolution in the First Committee in 1998 the Third Committee discussed a draft resolution introduced by the US and 38 other states entitled '[c]ombating the criminal misuse of information technologies'.[55] It was co-sponsored by the Russian Federation, but not China, with a further 19 Member States subsequently co-sponsoring it and was adopted without a vote on 22 January 2001.[56]

The key objective of this resolution was to establish a 'legal basis for combating the criminal use of information technologies'.[57] In attempting to realize this objective, the resolution had several key elements. First, it 'recogniz[ed] that the free flow of information can promote economic and social development, education and democratic governance'.[58] Second, it '[e]xpress[ed] concern that technological advancements ha[d] created new possibilities for criminal activity, in particular the criminal misuse of information technologies'.[59] Third, it 'recogniz[ed] the need for cooperation between States and private industry in combating the criminal misuses of information technologies'.[60] Lastly, it noted the value of 10 measures to combat the criminal misuse of information technologies including, inter alia, eliminating safe havens for those who criminally misuse information technologies,[61] law enforcement cooperation amongst concerned states,[62] information sharing,[63] the appropriate training of law enforcement personnel,[64] protecting the confidentiality, integrity and availability of data and computer systems and ensuring criminal misuse is penalized,[65] the preservation of and quick access to electronic data pertaining to particular criminal investigations,[66] the timely investigation and exchange of evidence of the criminal misuse of information technologies,[67] increasing public awareness of the need to prevent and combat, criminality in this area,[68] the designing of information technologies to help detect and prevent criminal misuse, trace criminals and collective evidence,[69] the development of solutions taking into account both the protection of

[54] Ibid., preamble.
[55] UNGA A/55/59, 16 November 2000.
[56] UNGA A/RES/55/63.
[57] UNGA A/57/529/Add.3.
[58] UNGA A/RES/55/63, preamble.
[59] Ibid., preamble.
[60] Ibid., preamble.
[61] Ibid., para. 1(a).
[62] Ibid., para. 1(b).
[63] Ibid., para. 1(c).
[64] Ibid., para. 1(d).
[65] Ibid., para. 1(e).
[66] Ibid., para. 1(f).
[67] Ibid., para. 1(g).
[68] Ibid., para. 1(h).
[69] Ibid., para. 1(i).

individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse.[70]

In 2001, a follow-up resolution – again, entitled '[c]ombating the criminal misuse of information technologies' – was introduced by the US and 73 other Member States, again including the Russian Federation but not China, with eight Member States joining later, and was adopted without a vote on 23 January 2002.[71] This took note of the measure set forth above, and again invited Member States to take them into account in their efforts to combat the criminal misuse of information technologies.[72]

Several resolutions, sponsored by Italy, titled '[s]trengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity' drew attention to the issue of 'cyber crime' and 'the use of new information technologies to abuse and exploit children', and 'invite[ed] the United Nations Office on Drugs and Crime to explore, within its mandate, ways and means of addressing these issues.'[73]

Lastly, the Third Committee adopted a resolution in 2013 titled '[t]he right to privacy in the digital age'.[74] The Edward Snowden revelations earlier in the year were a key reason for the adoption of this resolution. It was in this sense no surprise that its two key sponsors were Brazil and Germany, the leaders of which were the main victims of NSA surveillance operations. While it was first thought that the response of these two states would be 'an initiative on the international security front at the UN, in the end, Brazil and Germany decided it was best to present the matter in the context of respect for international human rights law and the right to privacy in particular.'[75] In this regard, the resolution emphasizes that 'illegal surveillance of communications, their interception and the illegal collection of personal data constitute a highly intrusive act that violates the right to privacy and freedom of expression and may threaten the foundations of a democratic society'.[76] The resolution recalls the obligation of states to 'ensure that measures taken to counter terrorism comply with international law' and recalls the privacy provisions of the International Covenant on Civil and Political Rights as well as the Universal Declaration of Human Rights.[77] The resolution calls upon states 'to take measures to put an end to violations of those rights'[78] and, in doing so, 'establish independent national oversight mechanisms capable of ensuring transparency and accountability of state surveillance of communications, their interception and collection of personal data'.[79] The resolution also requests that the UN High Commissioner for Human Rights reports 'on the protection of the right to privacy in the context of domestic and extraterritorial surveillance of communications, their interception and collection of personal data' and for a final

[70] Ibid., para. 1(j).
[71] UNGA A/RES/56/121.
[72] Ibid., para.2
[73] UNGA A/RES/63/195 (2008), UNGA A/RES/64/179 (2009), UNGA A/RES/65/232 (2010), UNGA A/RES/66/181 (2011), UNGA A/RES/67/189 (2012), and UNGA A/RES/68/193 (2013).
[74] UNGA A/RES/68/167.
[75] Meyer, supra n.7.
[76] UNGA A/RES/68/167, preamble.
[77] Ibid., preamble.
[78] Ibid., para. 4(b).
[79] Ibid., para. 4(d).

report to be submitted by the High Commissioner to the 2015 session of the General Assembly.[80]

While this was an undoubted important development in the context of cyber-security, it is also arguably true that '[t]he difficult political and legal questions underlying references to "unlawful interference with privacy" and constraints on "extraterritorial surveillance" will keep lawyers and diplomats busy for months if not years to come.'[81]

2.4. The Groups of Governmental Experts

Overall, and as demonstrated by the above sections, the UNGA has been active in regards to discussing principles, elements, good practice, etc regarding the behavior of Member States in the context of cyber security. However, what the above also arguably shows is that '[a]t the multilateral level, the UN will have to begin to address the cyber security issue in a more coherent fashion. The General Assembly can ill afford to have two deliberative streams (i.e. the First and Third Committee) acting in ignorance of one another.'[82] Indeed, '[t]he airing of declaratory policy at the annual General Assembly sessions should not substitute for purposeful action by states in more operational forums to tackle the pressing problems raised by destabilizing state conducted cyber operations.'[83] In this respect, the establishment of several Groups of Governmental Experts has been a significant development. Four GGEs have been established since 2004 that have examined the existing and potential threats from the cyber-sphere and possible cooperative measures to address them. The purpose of this section is to give an overview of the work of these Groups.

2.4.1. The First Group of Governmental Experts

The first GGE was established in 2004 by the UNGA's First Committee. The previous year, following on from a proposal by Russia,[84] Member States had:

> 'Request[ed] the Secretary-General to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct a study on [relevant international concepts aimed at strengthening the security of global information and telecommunications systems], with the assistance of a group of governmental experts, to be established in 2004, appointed by him on the basis of equitable geographical distribution and with the help of Member States in a position to render such

[80] Ibid., para. 5.
[81] Meyer, supra n.7.
[82] Ibid.
[83] Ibid.
[84] Russia noted in its report to the UN Secretary-General that 'the group will give the international community a unique opportunity to examine the entire range of issues involved'. 'Developments in the field of information and telecommunications in the context of information security', Report to the Secretary General, United Nations General Assembly, 58th Session, Addendum, A/58/373, 17 September 2003.

assistance, and to submit a report on the outcome of the study to the General Assembly at its sixtieth session.'[85]

Yet, over the course of three meetings the GGE failed to even find the smallest common denominator. It is perhaps quite unusual for such an outcome to occur at the UN where an activity is usually only initiated when it is clear before it starts that there is at least some smallest denominator that everyone can agree on.[86] Yet, the UN Secretary-General concluded in 2005 that it was due to 'the complexity of the issues involved' that 'no consensus was reached on the preparation of a final report'.[87]

A member of the Russia delegation at the GGE meetings claimed that '[t]he main stumbling block was the question of whether international humanitarian law and international law sufficiently regulate the security aspects of international relations in cases of "hostile" use of ICTs for politicomilitary purposes.'[88] The issue of whether existing law sufficiently regulated cyber threats is, as noted above, something that was an issue between Russia and the US. While Moscow urged the development of new norms and rules Washington was of the opinion that 'the law of armed conflict and its principles of necessity, proportionality and limitation of collateral damage already govern the use of such technologies.'[89]

Furthermore, the group was not able to agree on whether the discussions should focus on 'information content or information infrastructures'.[90] The US and EU were, as noted above, suspicious of the motives of Russia, more specifically that it was attempting to limit the freedom of information under the guise of increasing information and telecommunications security. Washington had clear concerns regarding any 'extension to governments of the right to approve or ban information transmitted into national territory from outside its borders should it be deemed disruptive politically, socially or culturally'.[91] Indeed, 'US apprehensions stemmed from concerns that authoritarian regimes would attempt to control the free flow of information using such a mechanism and restrict freedom of speech and expression.'[92]

However, despite the lack of agreement, 'the work of the GGE was not in vain as it successfully raised the profile of the relevant issues on the international agenda.'[93] In

[85] 'Developments in the field of information and telecommunications in the context of international security', UNGA A/RES/58/32, 8 December 2003, (on the report of the First Committee), para.4. The eventual GGE consisted of governmental experts from 15 States: Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, the Republic of Korea, Russia, South Africa, UK, and US. They unanimously elected Andrey V. Krutskikh of Russia as its Chairman.
[86] Maurer, supra n. 29, at 22.
[87] UNGA A/60/202, at 2.
[88] Maurer, supra n.29, at 22.
[89] 'Developments in the field of information and telecommunications in the context of information security', Report to the Secretary General, United Nations General Assembly, 59th Session, Addendum, A/59/116/Add.1, 28 December 2004.
[90] Fact Sheet – Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations Office for Disarmament Affairs, available at http://unoda-web.s3.amazonaws.com/wp-content/uploads/2013/06/Information_Security_Fact_Sheet.pdf
[91] 'Developments in the field of information and telecommunications in the context of information security', Report to the Secretary General, United Nations General Assembly, 59th Session, Addendum, A/59/116/Add.1, 28 December 2004.
[92] Prakesh and Baruah, supra n.2, at 2.
[93] Maurer, supra n.29, at 22.

addition, despite its notable failure the first GGE had initiated a certain momentum within the UN to consider cyber security. As such, during the sixtieth session of the UNGA, when the first GGE had been due to report, Member States adopted a resolution in which they

> 'Request[ed] the Secretary-General, with the assistance of a group of governmental experts, to be established in 2009 on the basis of equitable geographical distribution, to *continue* to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as the [relevant international concepts aimed at strengthening the security of global information and telecommunications systems], and to submit a report on the results of this study to the General Assembly at its sixty-fifth session'.[94]

The momentum that had developed as a result of the GGE initiative could only be increased by the fact that between the adoption of the resolution in 2005 requesting the establishment of a second GGE and its actual establishment in 2009 cyber-warfare had begun to make the headlines, with the DDoS attack against Estonia in 2007 and then, in 2008, with cyber conflict issues during the Georgian-Russian war.[95] Yet, these events did not mean that agreement amongst the second group of experts was assured. On the contrary, given the intensity of the situations and the parties involved things might equally have gone the other way. As it happened, however, a consensus began to emerge within the group with the inclusion in its report of some progressive steps.

2.4.2. The Second Group of Governmental Experts

Given the intervening events it was interesting that Estonia was a member of the second GGE,[96] having been the first state to suffer a massive DDoS attack. The GGE, having first convened in November 2009, met four times and in July 2010 issued the first successful report of a GGE.[97] It is clear that with the issuance of this report the UN took 'a step forward' in its regulation of cyber security.[98] In coming to a consensus the group was of the view that '[e]xisting and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century.'[99] Indeed, the threat was considered significant enough to pose a threat to 'international peace and national security'.[100] It recalled some of the existing efforts to

[94] UNGA A/RES/60/45, 8 December 2005, para. 4 (emphasis added).
[95] It is perhaps worth noting that the classification of these two incidents as examples of 'cyber-warfare' is not absolutely certain and is still dependent to an extent on the emerging consensus as to how to classify such incidents. See, in general, M. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).
[96] The eventual GGE consisted of governmental experts from 15 States: Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, Qatar, the Republic of Korea, Russia, South Africa, UK, and US. Mr. Andrey V. Krutskikh (Russia) was unanimously elected to Chair the Group.
[97] UNGA A/65/201.
[98] Hathaway *et* al, supra n. 8, at 49.
[99] UNGA A/65/201, at 2.
[100] Ibid.

combat the criminal use of information technology and noted the intention to create a 'global culture of cyber security'.[101]

In adding some flesh to the bones of this statement the report highlighted the 'dual use' character of cyber-space.[102] Indeed, the notion that the Internet is 'neutral' so that the use to which it is put and the consequences of this are dependent upon the intent of its user is a recurring theme of resolutions of the UNGA.[103] It also identified criminals, terrorists, and states as potential perpetrators of offences in cyber space while individuals, businesses, national infrastructures, and governments as potential victims.[104] Importantly, and arguably as a result of the events in Estonia, the report also acknowledged the attribution problem in connection with cyber attacks.[105] Given the impasse between the US and the Russian Federation in regards to the utility of existing international law in addressing cyber security or whether further rules and norms should be developed, it was perhaps of no surprise that the report equivocally noted that '[e]xisting agreements include norms relevant to the use of ICTs by States' although '[g]iven the unique attributes of ICTs, additional norms could be developed over time.'[106]

Arguably the most significant development in the report of the second GGE, however, were the five recommendations it made 'for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions'[107]:

- Dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructures;

- Confidence-building, stability, and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;

- Information exchanges on national legislation, national ICT security strategies and technologies, policies and best practices;

- Identification of measures to support capacity-building in less developed countries; and

- The elaboration of common terms and definitions in connection with information security

With these recommendations, the GGE had begun to cement four progressive themes of an emerging regulatory framework for cyber-security within the UNGA: common understandings of acceptable state behaviour, practical cooperation, confidence-

[101] Ibid., at 7. For more on this concept see section 2.2. above on the work of the Second Committee.
[102] Ibid., at 6.
[103] Ibid.
[104] Ibid.
[105] Ibid.
[106] Ibid., 8.
[107] Ibid., 8.

building measures, and capacity-building measures. Though perhaps vague, and as the UN Secretary-General noted the international community had 'only begun to develop the norms, laws and modes of cooperation needed',[108] 'these recommendations represent real progress in overcoming a long impasse between the United States and Russia over how to address cybersecurity issues. The cooperation may even suggest possibilities for a future multilateral treaty under the auspices of the United Nations, which Russia has been advocating for some time.'[109]

However, in 2010, the year in which the report had been issued and during which time the major WikiLeaks releases occurred and the Stuxnet attack against Iran had begun to unfold, a further important turning point arose in enabling the work of the UN to progress further and, in particular, establish further cooperation and normative understandings. Indeed, as noted above, it was at this point that the US decided to engage with other states to address the concerns it had over cyberspace and, in particular, for the first time to co-sponsor the Russian draft resolution in the First Committee.[110] Overall, the US's 'support of the UN resolution of 2009 (co-sponsored with Russia) as well as the successful completion of the second GGE were signs indicting this change.'[111] Furthermore, and in an attempt to build upon the substantial progress made in the report of the second GGE, the 2010 version of the resolution also included a new request to the Secretary-General to establish a further GGE in 2012 which was to submit a report at the 68th session of the UNGA in 2013.[112]

2.4.3. The Third Group of Governmental Experts

The third GGE was tasked with building upon the assessments and recommendations contained in the report of the second GGE and continuing to study existing and potential threats in the sphere of information security and possible cooperative measures to address them.[113] The GGE had three one week meetings, the first was held in New York in August 2012, the second in Geneva in January 2013, and the last in June 2013 in New York and issued its report on 7 June 2013.[114]

---

[108] Ibid., 4.
[109] Hathaway, supra n.8, at 50.
[110] UNGA A/RES/65/41, 8 December 2010. The resolution was sponsored by three dozen counties including China.
[111] Prakesh and Baruah, supra n.2, at 4.
[112] UNGA A/RES/65/41, para. 4. Similar to previous resolutions noted above, this paragraph stated that the UN Member states 'Request[ed] the Secretary-General, with the assistance of a group of governmental experts, to be established in 2012 on the basis of equitable geographical distribution, taking into account the assessments and recommendations contained in the above-mentioned report, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as [relevant international concepts aimed at strengthening the security of global information and telecommunications systems], and to submit a report on the results of this study to the Assembly at its sixty-eighth session.' Again, in 2011 the UNGA unanimously approved a resolution calling for a follow up to the last GGE (See UNGA A/RES/66/24).
[113] The following Member States participated in the GGE: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, UK and USA. Ms. Deborah Stokes (Australia) was unanimously elected to Chair the Group.
[114] UNGA A/68/98, 24 June 2013.

Forming a backdrop to the meetings of the GGE, in 2011 China, Russia, Tajikistan and Uzbekistan requested the UN Secretary-General to distribute to the 66th session of the UNGA an International Code of Conduct for Information Security which they had drafted, and which was an attempt to provide further regulation to cyber norms and governance.[115] In describing this document, China stated that it was 'a series of basic principles of maintaining information and network security which cover the political, military, economic, social, cultural, technical and other aspects.'[116] The Code suggested creating a multilateral mechanism in the form of a treaty to govern the Internet, something which, as noted above, had been vehemently opposed by the US. In response to the distribution of the Code of Conduct the US commented that '[a]t its heart, it calls for multilateral governance of the Internet that would replace the multistakeholder approach, where all users have a voice, with top-down control and regulation by states.'[117]

The Code reflected the concerns of its sponsor states, in particular it restricted its signatories from using 'ICTs including networks to carry out hostile activities or acts of aggression and pose threats to international peace and security. Not to proliferate information weapons and related technologies'.[118] However, the US was of the opinion that

> 'the draft Code appears to propose replacing existing international law that governs the use of force and relations among states in armed conflict with new, unclear, and ill-defined rules and concepts. Indeed, one of the primary sponsors of the draft Code has stated repeatedly that long-standing provisions of international law, including elements of jus ad bellum and jus in bello that would provide a legal framework for the way that states could use force in cyberspace, have no applicability. This position is not justified in international law and risks creating instability by wrongly suggesting the Internet is an ungoverned space to which existing law does not apply.'[119]

Furthermore, the Code suggested 'that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues'. The Code contained clauses curbing 'dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment'.[120] However, the US was clear that

> 'the introduction of a draft Code of Conduct for Information Security presented an alternative view that seeks to establish international justification for government control over Internet resources. … It would legitimize the

[115] UNGA A/66/359, see appendix.
[116] China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations, Foreign Ministry of People's Republic of China, 13 September 2011.
[117] Statement by Delegation of the United States of America, 'Other Disarmament Issues and International Security Segment of Thematic Debate in the First Committee of the Sixty-seventh Session of the United Nations General Assembly', 2 November 2013, available at http://www.state.gov/t/avc/rls/200050.htm.
[118] International Code of Conduct for Information Security, supra n.16.
[119] Statement by Delegation of the United States of America, supra n.117.
[120] International Code of Conduct for Information Security, supra n.16.

> view that the right to freedom of expression can be limited by national laws and cultural proclivities, thereby undermining that right as described in the Universal Declaration on Human Rights.'[121]

Ultimately, there was little support for the draft Code of Conduct which had little impact upon the report of the third GGE. However, the third GGE 'made significant progress on agreeing on some of the defining aspects' of cyber security.[122] As with the report of the second GGE and resolutions of the three committees of the UNGA, the report again noted the immense benefits brought by ICTs but also recognized their dual-use capabilities in that they could be used 'for purposes that are inconsistent with international peace and security'.[123] Similarly, it again noted the problem whereby the actors involved 'often act with impunity' and their malicious use of ICTs 'is easily concealed and attribution to a specific perpetrator can be difficult.'[124]

The report then focused on building upon the four progressive themes of the emerging regulatory framework for cyber-security within the UNGA: practical cooperation, common understandings of acceptable state behaviour, confidence-building measures, and capacity-building measures, and offered recommendations in respect to each including the important role of the private sector and civil society in any efforts. Where perhaps the report made most progress, however, was in its recommendations on 'norms, rules and principles of responsible behavior by States'. It was first noted that '[t]he application of norms derived from *existing* international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability.'[125] This was important, given the debate noted above between the US and the Russian Federation on this issue. If the report had left it at that question marks would have remained over what the GGE had meant when it referred to 'existing international law'. However, it went on to note that 'international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.'[126] This affirmation of the UN Charter, and perhaps in particular its rules on the non-use of force and self-defence, was significant. As the report noted further, 'State sovereignty and the international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.'[127]

On this subject, the report was also clear that 'State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments'.[128] This was a significant step that allayed some of the fears of Western states in regards to attempts by certain states to curb free use of the Internet. Lastly on the subject of the applicability of existing international law the report noted that

[121] Statement by Delegation of the United States of America, supra n.117.
[122] Prakesh and Baruah, supra n.2, at 5.
[123] UNGA A/68/98, at 6.
[124] Ibid.
[125] Ibid., at 8 (emphasis added)
[126] Ibid.
[127] Ibid.
[128] Ibid.

'States must meet their international obligations regarding internationally wrongful acts attributable to them.'[129]

However, the report was clear that further work was needed in this context. Indeed, it stressed, again, that '[c]ommon understandings on how such norms shall apply to State behavior and the use of ICTs by States requires further study.'[130] What was also notable was its recognition that '[g]iven the unique attributes of ICTs, additional norms could be developed over time', something which was arguably attributable to the efforts of some states to do just that.[131]

In his forward to the new report, the UN Secretary-General noted the 'broad recognition that misuse [of ICTs] poses risks to international peace and security'. However, he also specifically

> 'appreciate[d] the report's focus on the centrality of the Charter of the United Nations and international law as well as the importance of States exercising responsibility. The recommendations point the way forward for anchoring ICT security in the existing framework of international law and understandings that govern State relations and provide the foundation for international peace and security."[132]

On 27 December 2013, the UNGA unanimously adopted a resolution in which it took note of the outcome of the third GGE, although did not specifically reiterate the conclusion that existing international law applies to cyber space.[133] It also requested the Secretary-General to establish a further GGE that would report to the UNGA in 2015 and would study, in addition to threats and cooperative measures, the issues of the use of ICTs in conflicts and how exactly international law applies to state use of these technologies. The fourth GGE, with an expanded 20 experts, had its first meeting in New York in July 2014. The work of the GGEs, as such, continues. However, it is arguably the case that 'as the mandate of the group becomes more specific it will increasingly be challenged to find enough common ground on which to base a consensual report that adds value to what has already been produced.'[134]

It is not strictly accurate to claim that '[t]he conflicting currents of state views as evidenced in the First Committee debates are unlikely to be resolved via the GGE process', as, and as set above, the GGEs *have* adopted positions accommodating – albeit in a somewhat equivocal fashion – of the two main streams of views. However, it is still nonetheless the case that while the reports of the GGEs are of constructive use states will ultimately 'have to look to other multilateral, regional and bilateral forums to see what might be feasible in terms of confidence building measures and agreed norms of behaviour.'[135]

---

[129] Ibid.
[130] Ibid.
[131] Ibid.
[132] Ibid., at 4. The centrality of the UN Charter in this context has also been noted by several commentators: 'At the heart of the system is the UN Charter. It provides the legal framework which is the most accurate way to conceptualize the relationships between its various entities.' See Maurer, supra n.28, at 12.
[133] UNGA A/RES/68/243.
[134] Meyer, supra n.7.
[135] Ibid.

3. The United Nations Security Council

The UN Security Council (UNSC) is the only body able to create binding international law.[136] The UNSC's resolutions to date have not generally been concerned with aspects of cyber security. However, it has been active in the field of cyber-security, particular terrorism related aspects of it.

On 28 September 2001 the UNSC established the Counter-Terrorism Committee through UNSC resolution 1373 (2001) following the terrorist attacks of 11 September 2001.[137] The Counter-Terrorism Implementation Task Force was subsequently created by the UN Secretary-General in 2005 to ensure the coordination of the activities related to resolution 1373 (2001).[138] The Task Force went on to establish various Working Groups, one of which was concerned with Countering the Use of the Internet for Terrorist Purposes.

The Working Group's mandate is located within the 2006 United Nations Global Counter-Terrorism Strategy which includes a paragraph on exploring ways and means to '(a) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet; (b) Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard.'[139] While the Working Group was established in response to the 9/11 attacks it only later became linked to the broader cyber-security debate and today consists of various bodies, including Interpol, the Office of the High Commissioner for Human Rights and the United Nations Office on Drugs and Crime.

The Working Group has four goals:[140]

- identify and bring together stakeholders and partners on the abuse of the Internet for terrorist purposes, including using the web for radicalization, recruitment, training, operational planning, fundraising and other means;
- explore ways in which terrorists use the Internet;
- quantify the threat that this poses and examine options for addressing it at national, regional and global levels; and
- examine what role the UN might play.

The work of the Working Group began with a 'mapping exercise of relevant laws, conventions, resources and initiatives'.[141] This was based on information provided by various Member States, interviews conducted with various stakeholders, and publicly available information. A stakeholders' meeting was held in November 2008 which

[136] Art 25, UN Charter (1945).
[137] UNSC resolution 1373 (2001), para.6.
[138] This was endorsed by the UNGA in A/RES/60/288, at para.5.
[139] UNGA A/RES/60/288, section II, paragraph 12.
[140] See http://www.un.org/en/terrorism/ctitf/wg_counteringinternet.shtml
[141] Ibid.

'focused on creating common understanding among sectors which may have divergent ideas on countering use of the Internet for terrorist purposes, with the ultimate aim of determining what if any international action might be appropriate.'[142]

As a result, the Working Group published its first report in February 2009 which analyzed information provided by Member States and reflected the conclusions of the stakeholders' meeting.[143] Significantly, it concluded that at that moment there was no obvious terrorist threat in the area and that it was not obvious that it was a matter for action within the counter-terrorism remit of the UN. It did, however, outline ways suggested by Member States by which the UN could further contribute, including facilitating Member States sharing of best practices, building a database of research into use of the Internet for terrorist purposes, conducting more work on countering extremist ideologies, and creating international legal measures aimed at limiting the dissemination of terrorist content on the Internet.

In 2010 the Working Group began to build upon the work of the first report by addressing legal and technical challenges surrounding the efforts to counter the terrorist use of the Internet. The Working Group held two meetings with various stakeholders and published a report in May 2011.[144] The section on legal aspects distinguishes internet-specific and non-internet-specific laws and in doing so highlights that there have been three discernable trends:

- states that apply existing cybercrime legislation to terrorist use of the Internet
- states that apply existing counter-terrorism legislation to Internet-related acts; and
- states that have enacted specific legislation on terrorist use of the Internet.

Ultimately the report calls for a harmonization of national legislations by implementing regional instruments such as the Budapest Convention on Cybercrime or the Commonwealth Model Law on Cybercrime as well as international instruments such as the Convention against Transnational Organized Crime.

A third phase of the Working Group which began in 2011 has focused on the use of the Internet to counter the appeal of terrorism, specifically by analyzing the role of counter-narratives and effective messengers who can deliver these narratives. A report on this issue consisted of a summary of a conference held in Riyadh in January 2011 on 'The Use of the Internet to Counter the Appeal of Extremist Violence'.[145] The

[142] Ibid.
[143] United Nations Counter-terrorism Implementation Task Force, 'Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes', February 2009, available at http://www.un.org/en/terrorism/ctitf/pdfs/wg6-internet_rev1.pdf
[144] United Nations Counter-terrorism Implementation Task Force, 'Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects', May 2011, available at http://www.un.org/en/terrorism/ctitf/pdfs/WG_Compendium-Legal_and_Technical_Aspects_2011.pdf
[145] For the conference summary and follow-up/recommendations see http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_riyadh_conference_summary_recommendations.pdf

Conference 'focused on identifying good practices in using the Internet to undermine the appeal of terrorism, to expose its lack of legitimacy and its negative impact, and to undermine the credibility of its messengers'.[146] Key themes included 'the importance of identifying the target audience, crafting effective messages, identifying credible messengers, and using appropriate media to reach vulnerable communities.'[147] The Conference 'agreed that Governments might not always be best placed to lead this work and needed the cooperation of civil society, the private sector, academia, the media and victims of terrorism.'[148] Importantly, it was also agreed that '[g]iven the global nature of terrorist narratives and the need to counter them in the same space, there was a special role for the United Nations in facilitating discussion and action.'[149]

4. The Economic and Social Council

The third (and final) intergovernmental body of the UN to deal with issues of cyber-security is the Economic and Social Council (ECOSOC) which is the principal body for coordination, policy review, policy dialogue and recommendations on economic, social and environmental issues. ECOSOC has held a general interest in issues of cyber-security and related issues. In 2010, it opened its session with a briefing title 'Cyber security: emerging threats and challenges' and the following year it held a special event on 'Cybersecurity and development'.[150] However, it is in two of its functional commissions – the Commission on Crime Prevention and Criminal Justice and the Commission on Narcotic Drugs – where most activity has occurred, particularly in connection with the criminal use of cyber-space.

4.1. The Commission on Crime Prevention and Criminal Justice

The Commission on Crime Prevention and Criminal Justice (CCPCJ) was established by ECOSOC in 1992 and acts as the principal policymaking body of the UN in the field of crime prevention and criminal justice.[151] The first session of the Commission took place in 1992 with its work focusing on, as its name might suggest, crime and justice. In this respect, in 1998 the Commission requested the UNGA to include in the agenda of the Tenth Crime Congress a workshop on 'crimes related to the computer network'.[152] The following year, in 1999, the Commission also proposed a draft resolution for ECOSOC on the 'Work of the United Nations Crime Prevention and Criminal Justice Programme' requesting the Secretary-General to conduct a study on effective measures that could be taken at the national and international levels to prevent and control computer-related crimes in light of the workshop at the Tenth Crime Congress and to report on his results at CCPCJ's tenth session.[153]

---

[146] Ibid., at 1.
[147] Ibid.
[148] Ibid.
[149] Ibid.
[150] See http://www.un.org/en/ecosoc/julyhls/pdf10/gs_briefing_background_note.pdf and http://www.un.org/en/ecosoc/cybersecurity/summary.pdf respectively.
[151] ECOSOC resolution 1992/1, 6 February 1992. This was upon a request of the UNGA in A/RES/46/152
[152] E/1998/30-E/CN.15/1998/11.
[153] ECOSOC resolution 1999/23, 28 July 1999. For the report of the UN Secretary General see E/CN.15/2001/4.

The ultimate result of the consideration given to such crimes at the Tenth Crime Congress in 2000 was the adoption by the UNGA of the Vienna Declaration on Crime and Justice, in which Member States

> 'decide[d] to develop action-oriented policy recommendations on the prevention and control of computer-related crime, and we invite the Commission on Crime Prevention and Criminal Justice to undertake work in this regard, taking into account the ongoing work in other forums. We also commit ourselves to working towards enhancing our ability to prevent, investigate and prosecute high-technology and computer-related crime. [154]

At the CCPCJ's tenth session in 2001 a plan of action for implementing the Vienna Declaration was adopted including '[a]ction against high-technology and computer related crime' which recommended a series of national and international measures.[155] What was noticeable is that up until this point the focus was on computer crime as opposed to 'cyber' crime and security.[156] Indeed, it was only in the CCPCJ's 2002 report that the term 'cyber' was mentioned for the first time,[157] with a call for a UN convention on 'cybercrime' appearing in its 2004 report.[158] However, despite this activity it was only in 2010 that cybercrime became a prominent theme in its annual reports, with some speakers again bringing up the possibility of global convention against cybercrime.[159] It was also notable the extent to which cyber issues were prominent in the various issues discussed, including in the use of information technologies to exploit children, economic fraud and identity-related crime, and activities relating to combating cybercrime including technical assistance and capacity-building. Subsequent reports have included discussion on, for example, cybercrime in connection with the trafficking of cultural property,[160] and organized crime.[161]

Furthermore, ECOSOC and the UNGA requested the CCPCJ to establish, in line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, an open-ended intergovernmental expert group on cybercrime.[162] This group was to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

---

[154] Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, UNGA A/RES/55/59, 4 December 2000, para 18.
[155] E/2001/30/Rev.1-E/CN.15/2001/13/Rev.1
[156] Maurer, supra n.28, at 37.
[157] E/2002/30-E/CN.15/2002/14.
[158] E/2004/30–E/CN.15/2004/16. This was by the representative of Thailand.
[159] E/2011/30-E/CN.15/2011/21.
[160] E/2014/30 E/CN.15/2014/20.
[161] Ibid.
[162] ECOSOC resolution 2010/18; UNGA A/RES/65/230.

The first session of the group was held from 17 to 21 January 2011.[163] The UNGA noted with appreciation the work of the Expert Group and encouraged it to enhance its efforts to complete its work and to present the outcome of the study to the CCPCJ in due course.[164] The second session of the group was subsequently held from 25 to 28 February 2013.[165] The report includes discussion on issues such as legislation and frameworks, criminalization, law enforcement and investigations, electronic evidence and criminal justice, international cooperation and prevention.

4.2. The Commission on Narcotic Drugs

The Commission on Narcotic Drugs has focused on the use and abuse of the Internet only from a drug trafficking perspective in line with its functional mandate and did so as early as 1996.[166] In 2000 the Commission eventually adopted a resolution solely focused upon and titled 'Internet' which was brought to the attention of ECOSOC.[167] After the adoption of this resolution there was no further specific resolution on the internet or cyber issues, although repeated references were made to it as part of the Commission's discussions. However, in 2004, in reference to the 2000 resolution, the Commission prepared a draft resolution for ECOSOC on the 'Sale of internationally controlled licit drugs to individuals via the internet'.[168] In 2005, the Commission prepared a further resolution for ECOSOC titled 'Strengthening international cooperation in order to prevent the use of the Internet to commit drug-related crimes'[169] while in 2007 prepared a similar resolution on 'International cooperation in preventing the illegal distribution of internationally controlled licit substances via the internet.'[170]

5. Subsidiary Organs and Specialized Agencies

Aside from the intergovernmental bodies found within the UN Charter, there are several subsidiary organs and specialized agencies of the UN that work the field of cybersecurity. Although they are not expressly mentioned in the UN Charter they find their legal base there. Indeed, under Article 22 of the UN Charter '[t]he General Assembly may establish such subsidiary organs as it deems necessary for the performance of its functions' while Article 57 states that the 'various specialized agencies, established by intergovernmental agreement … shall be brought into relationship with the United Nations'. Of the many that exist, those key in the context of cybersecurity are the International Telecommunications Unit, the United Nations Institute for Disarmament Research, and the United Nations Office on Drugs and Crime. Although an extensive analysis of their individual roles and functions is beyond the scope of this chapter, their key functions in connection with cybersecurity will be briefly addressed.

[163] The report on that meeting is contained in document UNODC/CCPCJ/EG.4/2011/3.
[164] UNGA A/RES/67/189.
[165] The report on that meeting is contained in document UNODC/CCPCJ/EG.4/2013/L.1.
[166] E/1999/28/Rev.1.
[167] ECOSOC resolution 43/8.
[168] ECOSOC resolution 2004/42.
[169] ECOSOC resolution 48/5.
[170] ECOSOC resolution 50/11.

5.1. International Telecommunications Unit

The International Telecommunication Union (ITU) is the UN specialized agency for ICTs and has most responsibility for practical aspects of cyber-security. While it existed prior to the UN's founding in 1945 it subsequently joined the UN system as a specialized agency under Article 57 of the UN Charter. The ITU is not only a forum for discussion of cybersecurity issues, and thus advances the broad agenda set by its member states by focuses on specific initiatives, but also plays a key role role in setting technical standards.

The ITU Secretary-General launched the Global Cyber-Security Agenda in May 2007 which he described as being an 'international framework for cyber-security'.[171] A key part of this was the establishment of a high-level group of experts on cyber-security. The group held three meetings between 2007 and 2008 before publishing its Global Strategic Report in 2008,[172] which focused on five areas

- Legal measures;
- Technical and procedural measures;
- Organizational meausres;
- Capacity building; and
- International cooperation.

The recommendations of the group of experts to the ITU included

- developing model legislation for member states to adopt. The ITU has also developed a tool kit for cyber-crime legislation with sample language including explanatory comments which could form the basis for a harmonization of cybercrime laws;
- the creation of a 'Cyber-security Readiness Index';
- a framework for national infrastructure protection; and
- a conceptualization of what a culture of cyber-security could be understood to mean.

The ITU Secretary-General has taken on a particularly visible role in the cyber security agenda of the ITU. For example, at the 2010 World Telecom Development Conference in Hyderabad he proposed a 'no first attack vow' for cyberspace and that states 'should undertake not to harbour cyberterrorists and attackers in their country

[171] Maurer, supra n.28, at 30.
[172] See http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf

unpunished'[173] as well as drafting five principles of cyber-peace.[174] More recently in 2014, the ITU, along with the United Nations Children's Fund, and partners of the Child Online Protection Initiative, released updated Guidelines to strengthen online protection for children.[175] The ITU's initiatives in the context of Child Online Protection have 'been identified as an effort whose merit all states agree on and where trust can be built so that socialization effects could potentially produce positive spill over effects for the broader cyber-security agenda.'[176]

5.2. United Nations Institute for Disarmament Research

The United Nations Institute for Disarmament Research (UNIDR) is a voluntarily funded autonomous institute within the UN and generates ideas and promotes action on disarmament and security. It was one of the first UN bureaucracies to become involved in the issue of cyber-security and today its 'cyber work aims to carry out policy-focused capacity-building at the national, regional and multilateral level, as well as relevant research and analysis.'[177]

It has hosted two conferences relating to the discussions in the UNGA's First Committee. In 1999, the United Nations Department for Disarmament Affairs funded a two-day discussion meeting on 'Developments in the field of information and telecommunications in the context of international security'.[178] This conference was titled the same as the resolution introduced by Russia a year earlier and highlighted the different primary concerns that states had at that time. In 2008 Russia then funded a conference on 'Information & Communication Technologies and International Security' with the objective being '[t]o examine the existing and potential threats originating from the hostile use of information and communication technologies, discuss the unique challenges posed by ICTs to international security and possible responses.'[179] Today, as well as acting as a consultant to the GGEs, it has also hosted three cyber-security conferences, with the most recent in 2014 focusing on preventing cyber conflict.

5.3. United Nations Office on Drugs and Crime

Although cybersecurity is not formally within the domain of the United Nations Office on Drugs and Crime (UNODC), the Third Committee of the UNGA first requested for UNODC to become involved in technical assistance specifically relating to 'cyber crime' in 2008.[180] Member States officially requested UNODC to work on the use of the Internet for terrorist purposes for the first time at the 20th session of the Commission on Crime Prevention and Criminal Justice in April 2011 after it was first

[173] H. Wegener, 'Cyber Peace', in International Telecommunication Union and World Federation of Scientists, *The Quest for Cyber Peace*, January 2011, at 81, available at http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.
[174] Ibid., at 78.
[175] See http://www.itu.int/en/cop/Pages/guidelines.aspx.
[176] Maurer, supra n.28, at 30.
[177] See http://www.unidir.org/est-cyber.
[178] Maurer, supra n.28, at 28.
[179] Ibid
[180] UNGA A/RES/63/195

mentioned at the 19th session the year before. UNODC's Terrorism Prevention Unit contributed to a CTITF publication in 2012 for law enforcement investigators and criminal justice officers in connection with cases involving '[t]he use of the internet for terrorist purposes.'[181] It also took the lead in the 2013 Global Programme on Cybercrime which, as described above,[182] had been initiated by the CCPCJ and which aimed to assist Member States in strengthening existing national and international legal responses to cybercrime.

6. Conclusion

As with many areas of international life, events within the UN in the context of cyber security have arguably been overtaken by events on the ground, and the UN is struggling to catch up. The functioning of the UN in this or, indeed, any area of activity, is down to the will and ability of its Member States. While there remains a clear divide within the international community regarding the focus of any emerging regulatory framework and the underlying approach to govern cyberspace there has been a discernable shift in the will amongst states to take action to regulate activity within cyberspace in some form. Indeed, we have witnessed a distinct shift in activity, and perhaps momentum towards something substantial and meaningful being achieved within and by the UN.

Finnemore and Sikkink perceptively observed that '[n]orms do not appear out of thin air; they are actively built by agents having strong notions about appropriate or desirable behaviour in their community'.[183] While this chapter has only been able to offer a somewhat limited account of the activities of the UN and its Member States in this area, achievements can be seen in the number of UNGA resolutions adopted in various committees, the increasing number of sponsors of these resolutions, the progressive work of the GGEs, and the work on the issue of cyber security taking place across a range of organs, agencies and bodies. Furthermore, while certain concerns have been continuously repeated in the UNGA since 1998, in particular the need for advancing ICTs but with caution over their the dual-use nature, there has also been continuous, if sometimes sluggish, progress in finding common ground and elaborating upon it. Indeed, the need for practical cooperation between not just states but also between states and other stakeholders, the need to develop common understandings of acceptable state behaviour, and the need for confidence-building, transparency and capacity-building measures have become themes cemented most visibly within the discourse of the GGEs but are also discernable in the work of the other UN organs. Dialogue and communication between the various UN organs, bodies and groups now needs to be improved to enable further integrated concerted action and norm development.

Yet, it would be shortsighted to think that a regulatory framework can emerge solely within the forum of the UN. Indeed the UN itself has continuously noted the valuable efforts that have been made by international organizations and regional entities in this

[181] UNODC, 'The use of the internet for terrorist purposes' (United Nations, 2012), available at http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
[182] See section 4.1 above on the CCPCJ.
[183] M. Finnemore and K. Sikkink, 'International Norm Dynamics and Political Change', (1998) *International Organization* 894, at 896.

area, such as the African Union, ASEAN, the Council of Europe, ECOWAS, the EU, and the Shanghai Cooperation Organization, to name a few. However, states have also begun to act bilaterally in seeking to cooperate, come to common understandings, and build confidence and transparency between them in their operations in cyberspace. A good example of this is the working group on cyber security recently established between the US and China.[184] With US concerns regarding a new international regulatory framework in the form of a treaty still visible, the application of existing international rules and norms along with the existence of softer, albeit complex, regulation in this area looks set to continue for some time yet.

[184] BBC News, 'US and China to set up cyber security working group', 13 April 2013, available at http://www.bbc.co.uk/news/world-asia-china-22137950.